Click Passwords Under Investigation

Krzysztof Gołofit

Warsaw University of Technology, Faculty of Electronics and Information Technology
Nowowiejska 15/19, 00-665 Warsaw, Poland
Warsaw University, Faculty of Psychology, Stawki 5/7, 00-183 Warsaw, Poland
K.Golofit@elka.pw.edu.pl

Abstract. The paper explores one of the graphical authentication techniques as the possible solution to the most important problems of traditional passwords. The aim of this work is to bring together the technical (cryptological) and non-technical (psychological) awareness into the research on passwords (click passwords in this case). Security issues of any authentication mechanism (relying on knowledge) should not be considered without analysis of the human factor − since the users' human nature was identified as a source of major weaknesses of conventional authentication. The paper deals with techniques which reduce password space and make passwords guesses feasible. Four types of pictures areas (of graphical interfaces) were investigated in order to bring to light common vulnerabilities − three of them were identified as types, which the graphical keypads should avoid. Statistics exposing strong tendentiousness in click passwords selection were presented as well. Furthermore, the paper presents a discussion on several issues of title authentication with regard to traditional passwords and other graphical techniques.

Keywords: Click Passwords, PassPoints, Passlogix, graphical authentication, keypad, human factor, dictionary attacks, picture passwords.

1 Introduction

According to recent reports, there are many vulnerabilities typical for alphanumerical passwords. Statistics from actual systems and many researches show that the users are, as usual 'the weakest link in the security chain'. One of the major problems is the difficulty of remembering passwords, the other, ignoring security requirements. Users tend to create either too short passwords or passwords that though long enough are easy to guess. There is an informal rule stating that passwords which are easy to remember, are mostly also easy to break. According to Bruce Schneier [1], passwords' length distribution based on 34,000 users (Fig.1) shows that 65% of passwords have only up to 8 characters and almost 95% up to 10 characters. Other research [2] shows that only 17% of the inquired IT professionals use complex passwords (including letters, numbers and symbols) and 72% stated that they almost never or never change their access codes. Moreover, 52% of professional users tend to share their passwords and 65% of them have only one or two passwords to access the majority of services. A study of information contained within the passwords [3] shows that 66% of users' passwords are

J. Biskup and J. Lopez (Eds.): ESORICS 2007, LNCS 4734, pp. 343–358, 2007.

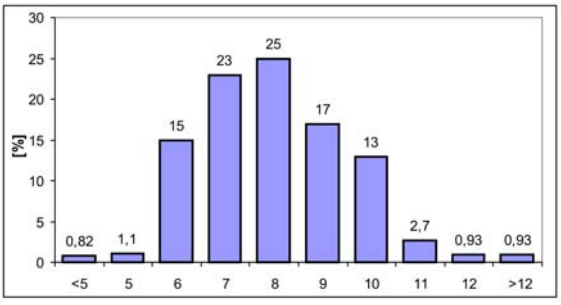

Fig. 1. Passwords' length distribution of 34,000 users (according to [1])

designed making use of personal characteristics thereof, where 32% contained names of people, places or things (three quarters of respondents used those for some passwords). Moreover, the common constructions involve full information in the passwords – 75%, partial – 13.5%, or combination – 7.5%. Almost all respondents reuse passwords – particularly 4.45 passwords are used in 8.18 systems. Once again, the adage that 'system fails when users pick the passwords for their own' finds many confirmations. On the other hand, strong passwords imposed on users bring no solution as well – because people cannot and/or would not remember strong passwords and will write them down instead. According to [4] and [5] we can say: there will be either about 80% remembered weak passwords (created by users) or strong passwords (generated by the system) in 80% written down.

Many alternative authentication solutions have been invented and developed to address the proper security level – in order to avoid weaknesses connected with knowledge-based methods. One group of techniques (involving a physical factor in the authentication process – called 'something you have') focuses on utilizing all kinds of tokens, one-time passwords, magnetic stripes and proximity cards, iButtons, cryptographic cards, etc. The other kind of research makes use of methods (called 'something you are') based on biometric information like fingerprints, voiceprints, the patterns of blood vessels on the eye retina, the topography of the eye iris, the geometry of the hand, facial patterns, DNA codes or even thoughts (cerebral waves). However, all of the aforementioned solutions have two significant disadvantages. First, they may become unacceptably expensive when a large number of users are involved. Second, access to the system is strongly dependent on the suitable interfaces – which makes such methods comparatively less universal (in the context of mobility) and in some cases, impossible to use. Additionally, biometrics is extremely vulnerable to a replay attack because the personal information cannot be changed.

In the past few years we have been observing a growing interest in graphical authentication techniques as an alternative to the alphanumerical passwords. There are significant advantages, which directly address well-known vulnerabilities of the traditional authentication mechanisms. Regardless of their application (in either weak or strong authentication), graphical methods might provide

higher level of security and/or lower implementation costs. On the contrary, as long as the discipline is still new, there is no knowledge about most possibilities of attacks – therefore weaknesses and drawbacks should be subject to thorough and careful investigation. This paper deals with the method called *Click Passwords* (*PassPoints*, *Passlogix* as well).

2 Related Work

By graphical authentication we mean those of knowledge-based methods, which include graphical aspect(s) in the authentication process. There are a few distinct grounds, which aroused the interest in graphical techniques. On one hand, graphical authentication methods are particularly useful for mobile devices or systems that have no keyboards [6]. On the other hand, there are methods resistant to *shoulder-surfing* attacks – enabling to log in 'in the crowd' (or in the places monitored by video cameras) [7], [8]; there are also obvious advantages coming from resistance to *malware* (malicious software) like *key-loggers* or *mouse-trackers* [9]. Notwithstanding, the leading inclination is still to construct authentication system, which will prevent from choosing trivial passwords and which will allow to remember passwords with the cryptographically proper length.

Click passwords. There are three techniques, known as *Passlogix* [10], *PassPoints* [11] (Fig.2) and *Click passwords* [12] based essentially on the same idea – users create passwords by choosing several arbitrary points in the picture. The login process requires performing the right sequence of clicked points with an assumed tolerance. One of the main problems is the need for picture's area's decomposition (arbitrary chosen polygons – groups of pixels), because of two simultaneous facts. First, there is a tolerance to inaccuracy of chosen points (screen pixels), second, we are not allowed to keep the coordinates of password points (only hash function results). As a consequence, a few schemes of picture decomposition were invented (some illustrated on Fig.3).

Fig. 2. Examples od graphical interfaces of *Passlogix*, [10] and *PassPoints*, [11]

The main goal of the click password systems (according to [12]) is to improve security (to maximize the password space). The password space through a proper chosen picture and through proper pixels assignments (to polygons) can reach very impressive values – even hundreds of thousands of points in the password base – from the technical point of view. On the contrary, there appears human tendentiousness that can significantly decrease the final space of choices – these issues are inspected farther in this paper. Nevertheless, we still lack (statistically) convincing evidence that click passwords can be easier to remember than the text based (assuming the same security level).

Fig. 3. Picture decomposition methods: regular grid (left), optimized *Voronoi tiling* (middle) and classification based on distance from arbitrary chosen points (right), [12]

Picture passwords. There is a group of methods where users choose and memorize a sequence of graphical elements (pictures) selected from a matrix of elements. With the name *picture passwords* we will usually identify interfaces consisting of large groups of elements (e.g. few dozens or a hundred) – although there are methods called *graphical PINs* that are usually used for small mobile devices (with few or several elements in the password base – Fig.4). Among picture passwords techniques there is a scheme called *Déjà Vu* – designed with non-describable abstract images [13], schemes based on images denoted 'Face' and 'Story' [14], thumbnail photos (quite similar to regular polygons of click passwords) [6] and others [15]. The general principle of those methods is essentially the same – the differences can be found in the graphical material, matrices

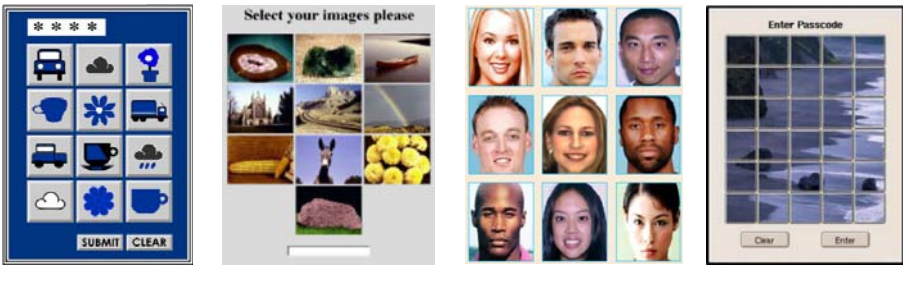

Fig. 4. Examples of *graphical PINs* (sources: [16], [17], [14], [6], respectively)

size (number of elements) and purpose. Those methods are particularly interesting (according to other research [9]) because of technical possibility of preventing users from choosing trivial passwords. On top of this, there is an approach to make the authentication process resistant to 'key logging' as well as to 'mouse tracking' software or hardware. Moreover, by choosing proper set of pictures, there was also proved (in [9]) the *picture password superiority*.

To get a basic idea of the scope of graphical authentication techniques there are a few more methods worth mentioning. A technique called *Draw-a-secret* (*DAS*) where the sequence of tap regions constitutes the password [18]. There are methods based on drawing the signature using mouse or light pen [19]. There are passwords (words) created as a response to automatically generated inkblots [20] (quite close to Rorschach's inkblots). There are other original techniques like *Pass-Go* − inspired by and based on the scheme of old Chinese game [21]. There is *RAF* (R*ecall a Formation*) scheme with two-dimensional picture passwords and *Mouse Motion* technique with intuitional mouse movements [15].

There is no psychological research, which can directly justify the superiority of graphical authentication. Although there is a phenomenon called *picture superiority effect* (term introduced by Nelson et al. in 1976, [22]) stating that pictures are much more likely to be remembered than words. However, in the experiments both pictures and words characterize the same concepts, e.g. word 'sun' vs. 'a drawing of the sun' − there is no knowledge about sequences of various pictures, various picture points or alphanumerical characters. There exists the *dual-coding theory* (introduced by Paivio, [23], [24]) saying that both visual and verbal information are processed differently and along distinct channels. Concrete concepts presented as pictures are encoded into both systems; however, abstract concepts are recorded only verbally. On the basis that separate information representations are processed in each channel there exists a part of Pavio's theory called *coding redundancy hypothesis*. It states that "memory increases directly with the number of alternative memory codes available for an item". It can be an argument in favor of click passwords when the users both name and picture their passwords − but also we do not know how single characters or their sequences will be coded.

Moreover, there are series of interesting researches, which can help to understand how to create efficient methods based on graphical materials. For example, study of what kind of information will be remembered over relatively long periods of time [25]; how people remember nonsensical material and what are the conditions to improve memory for pictures [26]; what is the role of prior knowledge in recognition [27]; what is the influence on memory when words and pictures are or are not recognized [28]; how we recognize pictures with or without additional details [29]; what is the influence of symmetry in the remembered material [30] and how can we manipulate with the colour (versus b&w), high versus low information, semantic versus sensory processing [31]. These (and many more that were omitted) can be only a clue to understand which factors should be taken into consideration when constructing the authentication mechanism, but none of them answers the question about strong and/or weak points of click passwords.

Nevertheless it shows how useful for the graphical authentication *mnemonics* (widespread nowadays) can be found.

3 Origins of Click Passwords Cryptanalysis

While the discipline is still in its infancy, there is no wide range of practical implementations and we have no direct observations on security of click passwords. We do not know much about possible attacks on the graphical authentication systems. There are a few hypotheses (below) that can result in disclosure of vulnerabilities of the picture material. An attempt has been made to identify universal weaknesses of the keypad images use in the authentication process. This knowledge can also result in proper design of the graphical interface by avoiding indicate regions. The hypotheses appear to be (entirely or partially) obvious, but as long as there are no appropriate results, we cannot refer to those as to vulnerabilities. Apart from effects affirmations, we would like to know about strength of those relations and on that ground conclude how dangerous potential attacks can be.

H1. First hypothesis is based on the belief that people would not choose points in the area where there are no footholds (spots) that can be clicked. Although we can imagine a scenario such that someone measures the distance from some objects and selects the password points in the *flat* area, even though the time and effort necessary to memorize such points make those choices quite unreliable. Thus, the first hypothesis states that there will be significant difference in choices between the regular and the *flat* area (first & fourth area on Fig.5).

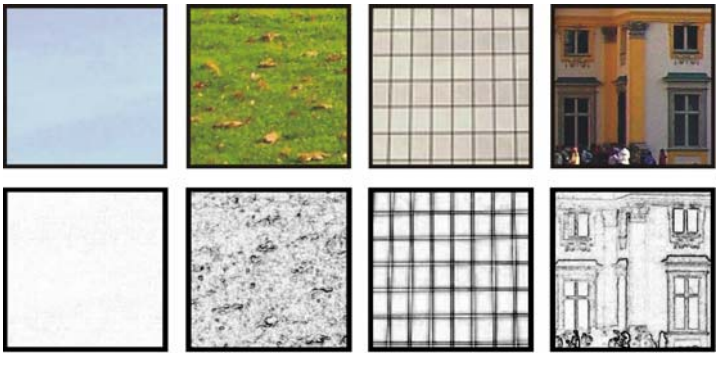

Fig. 5. Four types of examined areas (1: *flat*, 2: *irregular*, 3: *structural*, 4: *commonplace*) and below the same areas after high frequency filtering (edge detection)

H2. In the second case we deliver spots (footholds) that can be easily pointed in the picture. But there are two things making the memorizing difficult. First, there is no order (regular structure) − the points are chaotically spread. Second, the elements do not differ in particular way (easy to remember) from each other.

The suitable material for such research can be provided for instance by 'breaking waves of the sea' or 'leaves on the lawn' (as the second area on the Fig.5). High frequency filtering shows that there are many points to be clicked, but it is hard to believe that there is an efficient way to remember thus chosen points. Therefore, like in H1, we do not expect that points in the second area (on Fig.5) will be frequently chosen by the participants.

H3. The last of the examined areas is a *structural* region (third on Fig.5), for which there are three criteria. First, there should be footholds that can be easily pointed in the picture. Second, the elements must not have particular differences. And third, there should be a quite straightforward opportunity to memorize chosen points (as for example the number of row and column of such arrangement). In this area we expect to observe two effects (as H3 and H4). The first one determines H3 − just like before, there will be less interest in this area, compared with the regular one.

H4. According to H3 and the third *structural* area of Fig.5, when someone decides to make the password based on this region, the choices will be weak from the cryptographical point of view. The tendency (expected by H4) should be seen as a graphical arrangement of the password points − far from random one. Similar effect was observed in [9] (research on picture passwords), where participants selected row, column or diagonal of the picture passwords' elements (the more sophisticated ideas in passwords picking were based on e.g. moves of the chess knight).

We need one more clarification − what is the fourth area type in the Fig.5 − called *commonplace*. Commonplaces are the regions, which are the references areas for H1−H3 hypotheses in every keypad image. It is almost impossible to define 'what the areas are', but it is quite simple to define 'what the areas are not'. They are none of the previous areas (1−3 on the Fig. 5) − they can consist of those regions (as a matter of fact they have to), but only in small fragments (not in general).

Method. One of the main requirements when exploring human tendencies is to test a large number of subjects. In the described research the verification of the memorized passwords was given up. On one hand there was no control over malicious behaviour of the participants, but on the other hand, there was the possibility to put more subjects to the test. It had been certainly assured that the participants were convinced that in one week there would be a second part of the experiment (remembering and reproducing passwords).

Subjects. There were 301 experiment participants − students at the Warsaw University of Technology (Faculty of Electronics and Information Technology) in general from third up to 10^{th} semester of studies. Table 1 presents more accurate characteristics of participants groups.

Apparatus. Keypad I (*palace*) and Keypad II (*street*) were created with regard to the four hypotheses (H1−H4). First observations (of groups I and II − almost 80 participants) did not result in passwords placed in the third (*structural*) area

Table 1. Characteristic of the experiment participants with regard to keypad types

Groups:	I	II	III	IV	V	VI	Overall:
Number of Subjects:	46	32	36	69	60	58	**301**
Females / Males:	0/46	3/29	1/35	3/66	3/57	4/54	**14/287**
Semester of study:	3	6-10	5	4	4	6	**3-10**
Keypad I (palace):	26	7	3	24	19	20	**99**
Keypad II (street):	20	25	6	23	25	19	**118**
Keypad III (tower):	–	–	27	22	16	19	**84**
Rejected:	0	0	1	0	3	1	**5**

(there were too little choices). There was no chance to confirm the H4 hypothesis. To address the problem of lack of choices the third keypad was created (Keypad III – *tower*) where the *structural* area can be found nearly solely (on the sky) with the *commonplace* regions reduced to minimum (existing only as the edges of the office building). The boundaries and the percentage share of areas were plotted on every keypad illustration.
– Keypad I – *palace* (size 200mm x 120mm) – Fig. 6; area types: 1, 2, 4.
– Keypad II – *street* (size 200mm x 120mm) – Fig. 8; area types: 1, 3, 4.
– Keypad III – *tower* (size 120mm x 160mm) – Fig. 10; area types: 1, 3, (4).

Procedure. Instructions attached to the keypads asked the participants to choose and remember passwords consisting of seven picture points and the subjects were informed that the picture points should be remembered in the right order. There was no time restriction.

Results. All results (raw and processed) were presented graphically and numerically. The left charts of the Figures 7, 9, 10_b present hundreds of users' real choices (679, 812 and 581 – respectively) – but the same points (or points located in the direct neighbourhood thereof) aren't visible. More informative with regard to near placed choices are two-dimensional histograms (Figures 7, 9, 10_b on the right) – consisting of the 4mm x 4mm cells. The darker cell, the more choices were counted in favor thereof. Statistics for the area types (raw and based on the percentage share of areas in the image), statistics for the participants' choices (real and based on the percentage share of clicks according to the areas) and the densities of choices depending on the area types, were collected in Tables 2, 3, 4 (on the left) – respectively to the keypads.

The major results with regard to the H1 – H3 hypotheses are located in the last columns (Density) of aforementioned tables, where the number of choices were standardized for the sizes of areas. Thus, the outcomes indicate the mean numbers of choices per one square centimetre. The every keypad results show that each of the three area types (with density from 0.13 up to 0.69 choices in 1 cm^2) was chosen by participants definitely more rarely than the regular regions (with density from 5.19 up to 5.56 choices in 1 cm^2). It makes the *commonplace* about ten times more attractive a region. In consequence the strength of hypotheses relations were:

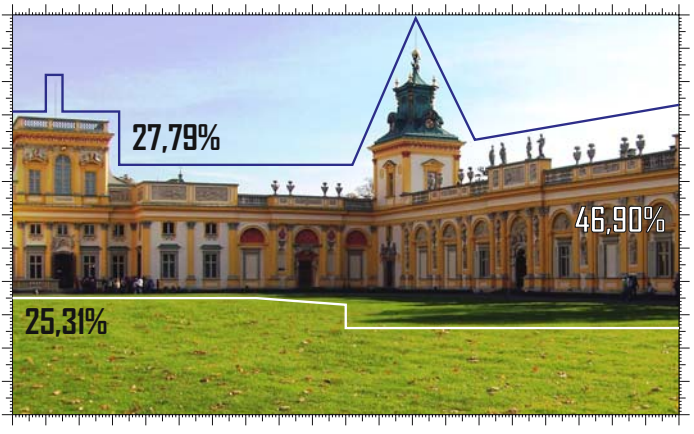

Fig. 6. Keypad I (*palace*); percentage share of areas: *flat*, *commonplace*, *irregular*. [32]

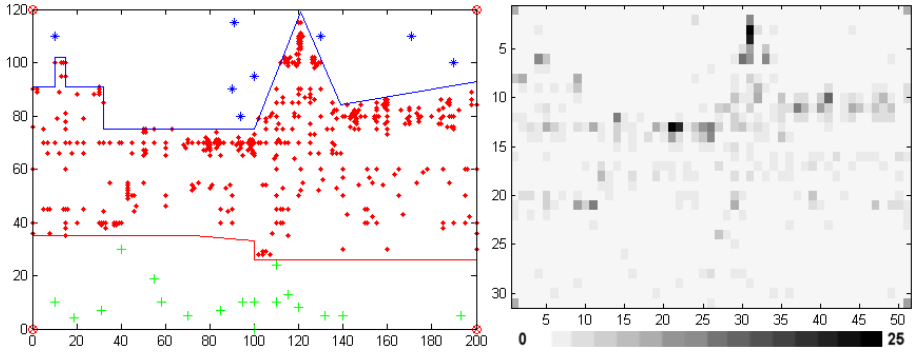

Fig. 7. Users' choices (left) and 51x31 '*heat map*' histogram (right) of the Keypad I

Table 2. Statistics of users' choices based on the Keypad I (*palace*)

Type of area:	Area		Choices		Density
	[cm^2]	[%]	[–]	[%]	[c-s/cm^2]
1: flat	66.70	27.79	9	1.33	0.135
2: irregular	60.73	25.31	19	2.80	0.313
4: commonplace	112.57	46.90	626	92.19	5.561
0: keypad corners	0	0	25	3.68	∞

Histogram (heat map) area				
1 %	3 %	5 %	10%	20%
Percent of users' choices				
[%]	[%]	[%]	[%]	[%]
29.0	53.9	67.0	83.5	100

H1 – 41.2x, 7.5x and 42,7x (respectively to the Keypads I, II, III);
H2 – 17,8x (in the Keypad II);
H3 – 11,5x and 9,1x (respectively to the Keypads II and III).
H4 – unfortunately there were only nine passwords among 83 and only 4 of

Fig. 8. Keypad II (*street*); percentage share of areas: *flat*, *structural*, *commonplace*. [33]

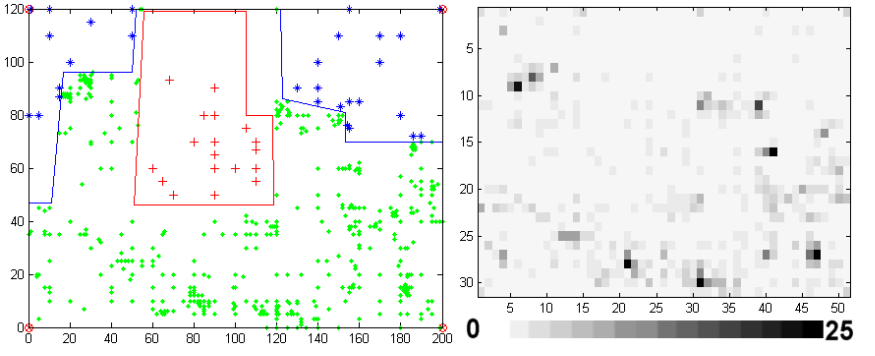

Fig. 9. Users' choices (left) and 51x31 '*heat map*' histogram (right) of the Keypad II

Table 3. Statistics of users' choices based on Keypad II (*street*)

Type of area:	Area		Choices		Density
	[cm^2]	[%]	[–]	[%]	[c-s/cm^2]
1: flat	53.72	22.38	37	4.56	0.689
3: structural	42.08	17.53	19	2.34	0.451
4: commonplace	144.2	60.01	749	92.24	5.194
0: keypad corners	0	0	7	0.86	∞

Histogram (heat map) area				
1 %	3 %	5 %	10%	20%
Percent of users' choices				
[%]	[%]	[%]	[%]	[%]
32.9	53.3	64.7	81.3	100

them inside the '*structural*' area (what makes about 11% and 5% of all choices respectively) that could confirm the H4 hypothesis (those passwords are illustrated on Fig.10 – top-right). Like before the subjects avoided the *structural* area (which was selected nine times more rarely than the reference region).

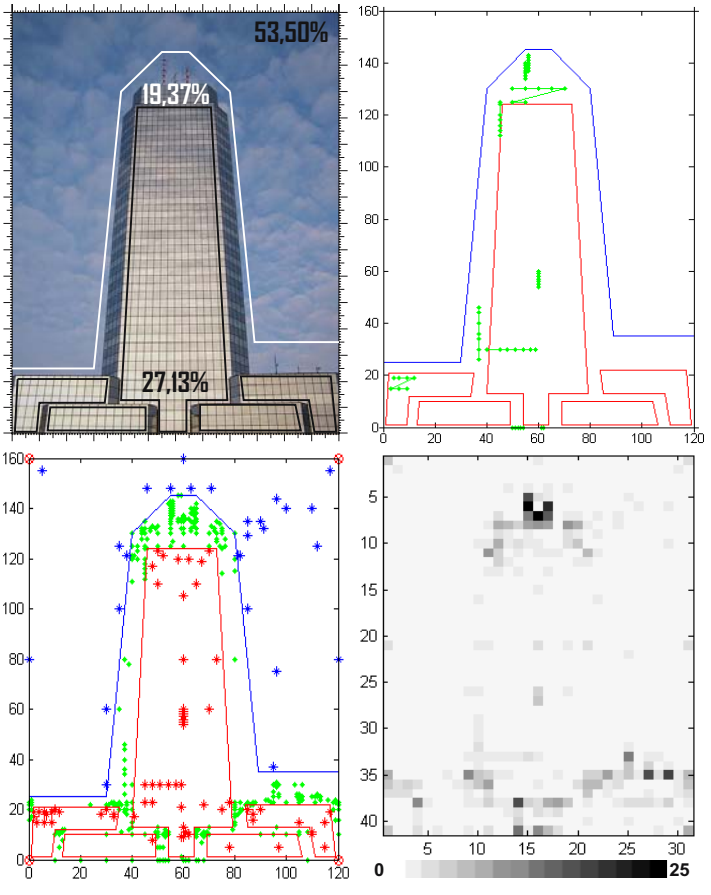

Fig. 10. Keypad III (*tower*) and the percentage share of areas: *flat*, *structural* and *block edges* (top-left); examples of passwords according to H4 (top-right); all users' choices (bottom-left) and 31x41 '*heat map*' histogram (bottom-right). [33]

Table 4. Statistics of users' choices based on Keypad III (*tower*)

Type of area:	Area		Choices		Density
	[cm^2]	[%]	[–]	[%]	[c-s/cm^2]
1: flat	102.7	53.5	30	5.16	0.292
3: structural	52.1	27.1	71	12.2	1.363
4: block edges	37.2	19.4	464	79.9	12.478
0: keypad corners	0	0	16	2.75	∞

Histogram (heat map) area				
1 %	3 %	5 %	10%	20%
Percent of users' choices				
[%]	[%]	[%]	[%]	[%]
32.9	59.4	72.6	88.8	100

Nevertheless there are also further observations – unintended but interesting findings reported in this paper. As the first of unforeseen results appeared the next type of users' choices – the corners of the keypads. The percentage shares

of all choices were 3.7%, 0.86% and 2.75% in accordance to the keypads' order (as presented in Tab. 2, 3, 4). The socond was farther tendentiousness.

There were several points (hot spots) within every keypad that were chosen especially often. A decent illustration of this effect are the '*heat maps*' (Figures 7, 9, 10_b – on the right) and statistics based on the 4mm x 4mm histograms presented in the Tables 2, 3 and 4 (on the right). Those tables demonstrate the general percentage of all keypad choices included in 1%, 3%, 5%, 10% and 20% of histograms areas - what corresponds to the right chart on Figure 11.

Two graphs (Fig.11) were presented to exemplify how strong the tendentiousness of the people's choices can be – the number of choices and percentage of all choices with regard to the percentage of keypads areas were illustrated. It can easily be noticed that every keypad includes more than 50% of all clicks (choices) in merely 3% of histogram areas. Moreover particularly different keypads are characterized by quite similar curves – such strong tendentiousness dramatically decreases password space and determines great vulnerability.

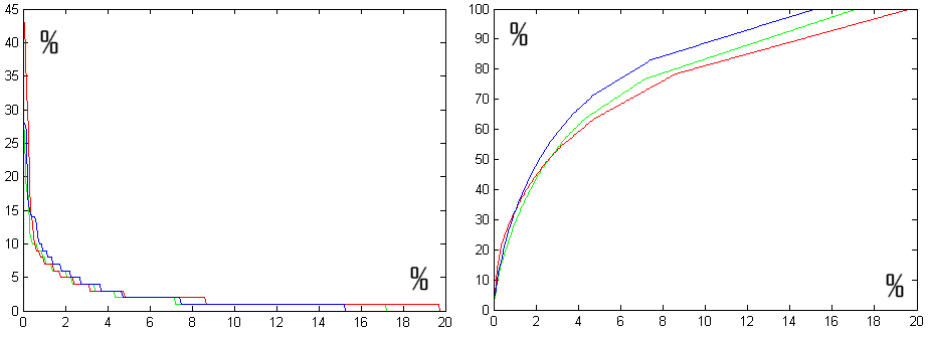

Fig. 11. Number of choices per one cell 4x4mm - decreasing ordered (left) and percentage of all choices (right), both with reference to the top 20% of histograms areas

4 Discussion of *Pros* and *Cons*

All presented results are only a small part of group of issues that should be taken into consideration before the practical use of click passwords (and related methods). This section is a compilation of conclusions of presented and so far not mentioned issues – regarding to the traditional alphanumerical passwords and picture passwords as well.

Advantages of Click Passwords

1. There are possibilities of significant enlargement of the password space of click passwords. In the traditional passwords, the base does not exceed one hundred (b^n – password space, b – base, n – password length,). Picture passwords offer the password base up to ten times larger. Technically, the click passwords space can be much greater than in the picture passwords

(hundreds of thousands) – but including strong tendentiousness in passwords selection, we do not know about real security strength of click passwords (that seems to be at picture passwords level).
2. Theoretically, there are possibilities of personalizing the passwords (what in most cases prevents from dictionary attacks) via individual interface pictures (using various images). However, there is a threat based upon tendentiousness of choices – for this reason every image should be tested at least in semi-large group of people.
3. There is a possibility to make the authentication process resistant to 'key logging' – which is obvious (due to not using the keyboard).
4. Sharing passwords with other users is much more difficult as well as noting passwords down or giving them away as a result of social engineering attack. While traditional passwords can be easily written down or spelled out, giving a click password out is very troublesome. This feature of click passwords is much better than in the picture passwords.
5. The password '*incrementation effect*' consisting in periodic, recurrent and obvious changes made to the passwords (e.g. a password change from "*11ESoRiCS06*" to "*12ESoRiCS07*)" can be neutralized. It is because there are no sequences or numbers when the keypad image was properly chosen (e.g. avoiding *structural* areas). And even when user changes only one point of the password – it is still hard to guess which one and where is the new one. What is more, there is always a way to force users to significantly change their passwords by exchange the keypad picture.
6. Likewise, rule "one system – one password" can be ensured by different keypad images in the systems where unique password codes are required.
7. There is a possibility for undemanding and inexpensive implementation (compared to biometric or cryptographic hardware).

Disadvantages of Click Passwords

1. Deterministic methods of picture decomposition will always result in some percentage of irritated or frustrated users. Even dealing with the best decomposition, there is always a probability (and statistically, certainty) that someone chooses password point in a polygon's border – and in half of the tries will fail the authentication process. As a matter of fact there is a usual trade-off between mentioned probability and the passwords space.
2. There is no technical possibility to prevent users from choosing trivial passwords (as distinct from picture passwords). The most important effort is to choose the proper keypad image. But only statistical analysis based on large (enough) group of people can confirm the right choice of the picture.
3. There is no possibility to make the authentication process resistant to 'mouse tracking' (as distinct from picture passwords). Every linear transformation of the keypad image can be easily cracked. Non-linear transformations require several more authentications but also can give the password (or its approximation) away.
4. More time needed to enter the password. Although we can expect shortening of the passwords (in comparison to alphanumerical passwords), we should

not expect better time performance in entering click passwords (even after the users have learnt the order of points).
5. Graphical interface is required − which means that the graphical authentication methods will be less universal (in terms of mobility) and troublesome in implementation (in comparison to traditional passwords).
6. There is no resistance to *shoulder-surfing* attacks − there is a better chance to observe the password entered on the screen than the alphanumerical password typed with traditional keyboard. (There are some picture passwords techniques dealing with *shoulder-surfing* attacks though).
7. There are many people who dislike: changes, giving up their habits, technical novelties, graphical interfaces (i.e. unix or linux users) and "compulsion to better life" (as in "we know what is better for you").
8. As for today, the discipline is still new and there may be many attacks, of which we cannot be aware at the present time.

5 Conclusions

In the paper four hypotheses were investigated in order to reveal universal weaknesses of the click password interfaces − three of them were proved right. The results determined three types of areas that will significantly decrease the password space. Additionally there was (unintentionally) distinguished strong tendentiousness of chosen passwords. Every of three keypad images indicates several common points that were chosen much more likely by the participants. It was shown that only 3% of the keypad image area includes more than 50% of all users' choices. On one hand, the possibilities of attacks on the authentication mechanism based on click passwords were exposed; on the other hand, the same results are useful as a way to improve security of this kind of authentication mechanisms.

A variety of technical and non-technical issues and conclusions, regarding click passwords, picture passwords and traditional passwords, was discussed in the paper. In order to understand peoples choices better and identify the potential causes of tendentiousness in click passwords selection, the eye tracking system will be further investigated.

References

1. Schneier, B.: Real-World Passwords. Crypto-Gram Newsletter (December 15, 2006)
2. Magalhaes, S.T., Revett, K., Santos, H.D.: Generation of Authentication Strings From Graphic Keys. International Journal of Computer Science and Network Security 6(3B), 240–246 (2006)
3. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Applied Cognitive Psychology 18, 641–651 (2004)
4. Carstens, D.S., McCauley-Bell, P., Malone, L.C., DeMara, R.F.: Evaluation of the Human Impact of Password Authentication Practices on Information Security. Informing Science Journal 7, 67–85 (2004)
5. Zviran, M., Haga, W.J.: User authentication by cognitive passwords: an empirical assessment. JCIT 5, 137–144 (1990)

6. Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R.: Picture Password: A Visual Login Technique for Mobile Devices. National Institute of Standards and Technology, NISTIR 7030
7. Zhi, L., Qibin, S., Yong, L., Giusto, D.D.: An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack. In: ICME. IEEE International Conference on Multimedia and Expo, IEEE Computer Society Press, Los Alamitos (2005)
8. Weinshall, D., Kirkpatrick, S.: Passwords You'll Never Forget, but Can't Recall. In: CHI. Proceedings of Conference on Human Factors in Computing Systems, Vienna, Austria, pp. 1399–1402 (2004)
9. Goofit, K.: Picture Passwords Superiority and Picture Passwords Dictionary Attacks (article seems to appear on SIS'07)
10. Paulson, L.D.: Taking a graphical approach to the password. Computer 35 (2002)
11. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Authentication using graphical passwords: Basic results. In: HCII 2005. Human-Computer Interaction International, Las Vegas (July 25-27, 2005)
12. Kirovski, D., Nebojsa, J., Roberts, P.: Click Passwords. Security and Privacy in Dynamic Env. 201, 351–363 (2006)
13. Dhamija, R., Perrig, A., Déjà Vu, A.: A User Study Using Images for Authentication. In: Proceedings of the 9th USENIX Security Symposium (2000)
14. Davis, D., Monrose, F., Reiter, M.K.: On User Choice in Graphical Password Schemes. In: Proceedings of the 13th USENIX Security Symposium, pp. 151–164 (August 2004)
15. Suo, X.: A Design and Analysis of Graphical Password. M.Sc. thesis, Georgia State University (2006)
16. Tricerion: The Usability of Picture Passwords (April 2007), `http://www.tricerion.com/`
17. Angeli, A., Coventry, L., Johnson, G.I., Coutts, M.: Usability and user authentication: Pictorial passwords vs. PIN. In: McCabe, P.T. (ed.) Contemporary Ergonomics, pp. 253–258. Taylor & Francis, London (2003)
18. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., Rubin, A.: The design and analysis of graphical passwords. In: USENIX (1998)
19. Syukri, A.F., Okamoto, E., Mambo, M.A: User Identification System Using Signature Written with Mouse. In: Boyd, C., Dawson, E. (eds.) ACISP 1998. LNCS, vol. 1438, pp. 403–441. Springer, Heidelberg (1998)
20. Stubblefield, A., Simon, D.R.: Inkblot Authentication. Microsoft Technical Report MSR-TR-2004-85 (2004)
21. Tao, H.: Pass-Go, a New Graphical Password Scheme. Master thesis, Univeristy of Ottawa, Ontario, Canada (June 2006)
22. Nelson, D.L., Reed, U.S., Walling, J.R.: Picture superiority effect. Journal of Experimental Psychology: Human Learning & Memory 2, 523–528 (1976)
23. Paivio, A.: Imagery and verbal processes. Holt, Rinehart & Winston, New York (1971)
24. Paivio, A.: Mental representations: A dual-coding approach. Oxford University Press, New York (1986)
25. Mandler, J., Ritchey, G.: Long-term memory for pictures. Journal of Experimental Psychology: Human Learning and Memory, 386–396 (1977)
26. Bower, G.H., Karlin, M.B., Dueck, A.: Comprehension and Memory For Pictures. Memory and Cognition 3, 216–220 (1975)

27. Long, D.L., Prat, C.S.: Memory for Star Trek: The Role of Prior Knowledge Recognition Revisited. Journal of Experimental Psychology: Learning, Memory, and Cognition 28(6), 1073–1082 (2002)
28. Kroll, J.F., Potter, M.C.: Recognizing words, Pictures, and Concepts - A Comparison of Lexical, Object, and Reality Decisions. Journal Of Verbal Learning And Verbal Behavior 23, 39–66 (1984)
29. Pezdek, K., Maki, R., Valencia-Laver, D., Whetstone, T., Stoeckert, J., Dougherty, T.: Picture Memory: Recognizing Added and Deleted Details. Journal of experimental psychology. Learning, memory, and cognition 14(3), 468–476 (1988)
30. Attneave, F.: Symmetry, Information and Memory Patterns. American Journal of Psychology 68, 209–222 (1955)
31. Childers, T.L., Houston, M.J.: Conditions for a Picture-Superiority Effect on Consumer Memory. Journal of Consumer Research 11, 643–654 (1984)
32. Jakub600, Wilanów: Graphical material (processed and published with author's consent) All rights reserved, `http://www.obiektywni.pl`
33. CorelDRAW: Clipart and Photos. Graphical material used for research comes from CorelDRAW distribution (license for ISE PW). All rights reserved